TRIBUNAL REGIONAL ELEITORAL DO PARA

RUA JOÃO DIOGO, 288 - Bairro CAMPINA - CEP 66015902 - Belém - PA

ESTUDOS PRELIMINARES

(AQUISIÇÃO DE BENS)

ANÁLISE DE VIABILIDADE DA CONTRATAÇÃO

1. CARACTERIZAÇÃO DA DEMANDA

1.1. Identificação das necessidades de negócio

A Tecnologia da Informação tornou-se para a administração pública, em especial o judiciário federal, ferramenta essencial para otimização das atividades administrativas, possibilitando a modernização da prestação jurisdicional, mediante a implantação de procedimentos mais ágeis, seguros, integrados e acessíveis aos jurisdicionados e ao cidadão. Tal fato decorreu da transformação digital, que nos últimos anos tem alavancado a digitalização dos processos de trabalho, proporcionando o alcance de diversas metas, consolidada em dois aspectos principais: a capacidade de lidar com o gigantesco número de informações, com o armazenamento e processamento de dados, recurso sem o qual o gerenciamento das informações já teria se tornado inviável e insustentável; e, em segundo lugar, por meio de tecnologias e sistemas de informação baseados na Web, que deram suporte à consecução da transparência e da razoável duração do processo legal por meio da digitalização dos processos de trabalho, assegurando a celeridade da tramitação processual, oferecendo como resultado a eficiente prestação jurisdicional. Os recursos, tecnologias e serviços computacionais, tornaram-se a base para a garantia da confiabilidade, integridade e disponibilidade das informações custodiadas.

Com a ampliação da disponibilização das soluções baseadas em serviços e protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure), tanto para acessos externos e internos, os aplicativos da Web passaram a suportar uma ampla gama de funções críticas em diversos sistemas que sustentam os negócios, incluindo sistemas de recursos humanos, transparência e consulta processual, sistemas que suportam processos administrativos e judiciais, dentre outros. Entretanto, estes meios tornaram-se uma brecha para ataques, pois os hackers não só podem invadir e roubar os dados das organizações por meio de e-mails maliciosos, programas infectados ou links duvidosos, como também oferecer perigo por meio do tráfego online até o site ou aplicativo corporativo. Portanto, torna-se necessário a ampliação da segurança, uma vez que os sistemas online podem conter potenciais vetores que se tornam alvos para a exploração de falhas, resultando nos conhecidos ataques cibernéticos.

Deste modo, milhares de sites são invadidos todos os dias devido a configurações incorretas ou códigos vulneráveis. Neste contexto, estudos recentes apontam que cerca de 50% das aplicações Web disponíveis na Internet possuem pelo menos uma vulnerabilidade de alta criticidade, como SQL Injection. Se for levado em consideração o nível de risco médio, cerca de 90% das aplicações publicadas na Web podem ser consideradas vulneráveis. Ainda segundo relatórios especializados, a vulnerabilidade de Cross-Site Scripting (XSS) é uma das mais comuns e mais exploradas (representando cerca de 30%) em aplicações Web. Além de ser frequente, em alguns casos, a exploração da vulnerabilidade XSS permite ao atacante acessar recursos e dados privados. Além das vulnerabilidades conhecidas, existem ainda as chamadas falhas do tipo "Zero Day", que se trata de uma vulnerabilidade de segurança desconhecida do público e do próprio desenvolvedor de um software. Isso significa que, a partir do momento em que a falha é detectada, o fabricante do software tem efetivamente “zero dias” para produzir uma atualização que corrija o problema, impedindo a exploração por criminosos antes da aplicação do patch que corrige a vulnerabilidade. Por outro lado, por motivos, algumas vezes, intrínsecos ao código da aplicação, não é possível aplicar o patch sem a necessidade de reescrever parte ou todo o sistema. Portanto, existe a necessidade de adoção de mecanismos para mitigação do risco de ataques, enquanto a equipe de desenvolvimento está realizando ajustes na aplicação para possibilitar a aplicação do patch.

Como uma forma de contribuir para o estudo e proteção dos ambientes no cenário crítico das aplicações Web disponíveis na Internet, especialistas em segurança da informação criaram a fundação OWASP (The Open Web Application Security Project). A entidade tem como principal objetivo disseminar conhecimento sobre segurança de aplicações Web disponíveis na Internet. Além disso, a OWASP também mantém um ranking tri-anual das 10 vulnerabilidades mais recorrentes em sistemas Web, conhecido como OWASP Top 10.

Objetivando mitigar o risco de ataques cibernéticos, por meio da estratégia de diminuição da superfície de ataque, uma das ferramentas que tem sido utilizada na proteção de aplicações Web são os **Web Application Firewalls (WAFs)**. Um WAF é um serviço de segurança implementado entre o cliente (e.g., navegador/browser) e a aplicação (e.g., sistema PHP rodando num servidor Web Apache). A função do WAF é interceptar, inspecionar e processar as requisições entre o cliente e a aplicação. A partir de um conjunto de regras, ele classifica as requisições em maliciosas (que são geralmente bloqueadas) e não-maliciosas, isto é, que são encaminhadas até a aplicação. Apesar de ser um estratégia de proteção conhecida há alguns anos, a importância dos WAFs tem crescido rapidamente no contexto atual, onde ciber ataques, que exploram as vulnerabilidades mais recorrentes de aplicações Web, têm crescido exponencialmente.

Atualmente, a arquitetura de segurança implantada na maioria dos Tribunais Eleitorais está baseada principalmente em Firewall NG (Next Generation) e firewalls tradicionais. Firewall NG (Next Generation) realizam inspeção profunda de pacotes (verificação do conteúdo do pacote de dados), podendo incluir outras tecnologias, como os Filtros de URFs e sistemas de prevenção contra invasão (IPSs), que trabalham para interromper automaticamente os ataques contra a rede. Além disso, outros TREs também utilizam soluções baseadas em *endpoint*, como soluções de antivírus. A referida arquitetura vem até agora atendendo às necessidades básicas, no entanto, apresenta restrições quanto à capacidade e proteção de aplicações em camada 7. Resta claro, portanto, a necessidade de adequação da

infraestrutura às novas ameaças digitais, sobretudo frente ao número de acessos e ampliação dos serviços externos providos pela Justiça Eleitoral.

1.2. Motivação (Art. 18, § 3º, II, a)

Com base nas diretrizes definidas na Estratégia Nacional de Cibersegurança, definidas pelo Tribunal Superior Eleitoral (TSE), vários investimentos em Tecnologia da Informação e Comunicação (TIC) estão sendo realizados para modernizar sua infraestrutura de TIC com a finalidade mitigar o risco de ataques cibernéticos.

Dessa forma, visando ao alinhamento estratégico e ganho em escalabilidade, disponibilidade, confiabilidade na entrega dos serviços prestados à sociedade, o TRE-PA pretende adquirir solução de Application Delivery Controller (ADC) que compreende funções de balanceamento de aplicações e tráfego e firewall de aplicações.

Uma das funções realizada pela referida solução é o balanceamento de aplicações, que permite o aumento da disponibilidade, fazendo com que os acessos sejam distribuídos entre os recursos de infraestrutura, de maneira a otimizar seu uso.

Outra função que pode ser realizada pelo WAF é o de firewall de aplicações (mecanismo de segurança), que aumentará a disponibilidade dos sistemas essenciais, acrescendo uma série de funcionalidades à segurança de TIC do TRE-PA, mapeando acessos específicos que acontecem na camada de aplicação, com o objetivo de garantir a proteção adequada aos sistemas e dados armazenados no Data Center do Tribunal.

Propõe-se, para tanto, a aquisição de Solução de Segurança da Informação – Firewall de Aplicação Web (WAF), visando à segurança e o bom desempenho das atividades no âmbito desta Justiça Especializada. Conforme exposto, a aquisição fundamenta-se em razão da necessidade de mitigar os inúmeros riscos inerentes aos sistemas informatizados disponibilizados no Portais Internet e Intranet do Tribunal e, consequentemente, aumentar a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

A motivação da contratação se dá, portanto, com base nas seguintes necessidades:

- No quesito segurança, pelo oferecimento de uma camada adicional de defesa, protegendo os servidores que hospedam aplicações Web, e executando funções de segurança de proteção dos servidores internos contra ataques por usuários da internet;
- No quesito performance, pela melhoria de acesso às aplicações dos sistemas judiciários, através do balanceamento de carga;
- Ampliar o controle de perímetro, por meio da inspeção e análise contínuo de tráfego das aplicações;
- Aprimorar os mecanismos de monitoramento e detecção de ataques;
- Proporcionar a prevenção e mitigação de ameaças cibernéticas;
- Contribuir para a redução da superfície de ataques cibernéticos da Justiça Eleitoral.

1.3. Objetivos a serem alcançados por meio da contratação (Art. 18, § 3º, II, b)

- Garantir que o acesso lógico aos ativos seja gerenciado e protegido, por meio de mecanismos de segurança de perímetro;
- Tornar a infraestrutura da Justiça Eleitoral mais segura e confiável;
- Prover resiliência ao ambiente de produção;
- Assegurar a redundância adequada ao acesso de Sistemas hospedados pelo Tribunal.

1.4. Premissas Gerais da Contratação

- A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise);
- A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução;
- A CONTRATADA deverá ofertar a solução na modalidade de Appliance Físico e Appliance Virtual;
- A contratação deverá fornecer implantação da solução no ambiente do Tribunal e treinamento EAD;
- A CONTRATADA deverá ofertar Garantia do Fabricante por 60(sessenta) meses. A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da versão fornecida do sistema operacional.

1.4. Benefícios resultantes da contratação (Art. 18, § 3º, II, c)

- Modernizar a infraestrutura de Segurança da Informação;
- Aumentar a disponibilidade, integridade e confiabilidade dos sistemas do Tribunal.

1.5. A demanda está incluída no rol de contratações previstas e aprovadas no Plano de Contratações de STIC ? (Art. 12, § 7º, II)

- Esta ação está prevista Plano de Contratações TRE-PA 2022 PORTARIA Nº 20790/2021 TRE/PRE/DG/SA/GABSA: Item 22 - SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB(WAF) / ANEXO IV CONTRATAÇÕES DE TIC - ORDINÁRIO (evento 1417657).

1.6. Identificação do público-alvo (unidades orgânicas, autoridades, servidores, outros) relacionadas à contratação:

- Magistradas, magistrados, servidoras, servidores, colaboradoras e colaboradores internos e externos, ocupantes de cargo em comissão sem vínculo efetivo, membros do Ministério Público, e quaisquer outras pessoas que fazem uso ou tenham acesso aos sistemas informatizados disponibilizados pelo Portal Intranet do Tribunal;
- Sociedade em geral que faz uso dos serviços publicados no Portal Internet do Tribunal.

1.7. Benefícios esperados da contratação

Dentre os resultados gerais esperados, enumeramos os seguintes:

- Com a solução proposta será possível reduzir os riscos existentes, relacionados à publicação de sistemas informatizados na Internet e intranet.
- A solução está associada a aplicação de controles para mitigação de riscos, em conformidade com a norma ABNT NBR ISO/IEC 27005:2019.
- Mitigação de ataques cibernéticos à infraestrutura Web conhecidos e prevenção de ataques Zero Day
- Melhorar a conformidade em relação às normas e boas práticas de Segurança da informação;
- Contribuir na eficácia e segurança de Aplicações Web;
- Padronizar e auditar políticas de segurança da informação, quanto ao acesso a sistemas e informações sensíveis;
- Aumento da eficiência operacional.

1.8. Consequência(s), caso não haja atendimento da necessidade:

- Entre os fatores que contribuem para o aumento dos ataques cibernéticos está a exploração de vulnerabilidades de aplicações Web. Desse modo, caso não seja atendida esta demanda o Tribunal estará vulnerável aos seguintes riscos:
  - Aumento do risco de vazamento de dados sensíveis;
  - Interrupção de serviços essenciais ao negócio do Tribunal (por exemplo, indisponibilidade de sistemas e serviços como o SEI, intranet, demais serviços online);
  - Dano à reputação;
  - Não conformidade à legislação vigente associada à proteção de dados;
  - Dificuldade de investigação e preservação de evidências, em casos de incidentes de segurança da informação e/ou Crise Cibernética.

1.9. Alinhamento da necessidade ao Planejamento Estratégico de TI do TRE-PA:

A presente contratação encontra-se alinhada aos objetivos do Planejamento Estratégico de Tecnologia da Informação (PETI) do TRE-PA:

- OBJETIVO 2 - Garantir a modernização dos serviços e infraestrutura de TI
- OBJETIVO 4 - Aperfeiçoar as práticas de gestão e governança de TI
- OBJETIVO 7 - Implementar o processo de segurança da informação

Por fim, esta aquisição está em conformidade ao ANEXO VI (Gestão de Identidade e de Controle de Acessos) da Portaria Nº 162 de 10/06/2021 que Aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

1.10. Justificativas da Contratação

Com o crescimento dos ataques cibernéticos e espionagem virtual aos quais as empresas privadas e os órgãos da administração pública, especialmente o judiciário, têm sido vítimas, torna-se urgente a necessidade de adoção de mecanismos de segurança da informação e a utilização de recursos de inspeção e proteção do tráfego de dados que auxiliem, de forma proativa, a prevenção e proteção dos sistemas, ante às vulnerabilidades encontradas em diversos vetores – redes (perímetro), sistemas e aplicativos, servidores de aplicação, e infraestrutura de orquestradores de containers.

O TRE-PA trata diariamente um grande volume de dados sensíveis e processos de trabalho, para os quais precisa garantir confidencialidade, disponibilidade e integridade destas informações. De outro lado, a partir da ampliação da transformação digital e a disponibilização das soluções de software baseadas nos protocolos que constituem a Web, principalmente, HTTP (HyperText Transfer Protocol) e HTTPS (HyperText Transfer Protocol Secure) para acessos externos e internos, respectivamente, via Internet e Intranet, tornou-se necessário reduzir a superfície de ataque, ampliando a segurança da informação deste egrégio Tribunal, uma vez que tais aplicações são vetores potenciais para exploração de falhas, principalmente ao se considerar a complexidade das arquiteturas de softwares e plataformas utilizadas.

Neste cenário, a maioria das ameaças explora vulnerabilidades existentes em aplicações. Por isso, é necessária a contratação de uma solução que possa, de forma customizada ao ambiente, interceptar e mitigar o risco inerente aos sistemas. O alvo dos atacantes geralmente são vulnerabilidades em sistemas desatualizados, legados ou com falhas no desenvolvimento. Por meio dessas brechas, são realizados diversos tipos de ataques, visando à espionagem, ao vazamento de dados, ao roubo ou sequestro de informações, ou ainda à quebra de integridade e disponibilidade do ambiente.

Além do risco de vazamento de dados sensíveis, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem do Tribunal. Para que seja alcançado o nível de segurança exigido nos dias atuais, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Diante disso, Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), no Eixo Estruturante E3: Ferramentas Automatizadas (Ferramentas de Segurança de Borda), apontou a necessidade de contratação e implantação de solução de segurança WAF que permita realizar a proteção das aplicações da Internet/Intranet. A solução WAF, ou Firewall de Aplicação Web, é uma solução que fica entre o site ou aplicativo e o restante da internet e a rede interna, funcionando como uma barreira que bloqueia e protege o ambiente de aplicações contra ataques de Hackers, Spammers, DDoS, Injeções SQL, proteção contra captura de dados sensíveis e roubo de credenciais, prevenção à atividade de robôs (bots) maliciosos e muito outros tipos de ataques cibernéticos conhecidos.

Adicionalmente, considerando a necessidade de redução da complexidade da operação e a consolidação dos serviços para as aplicações, bem como o crescente uso de soluções e arquiteturas de software baseadas em contêineres, torna-se necessário que a solução pretendida inclua solução de balanceamento de carga e que a mesma seja integrada ao ambiente de contêineres, visando equalizar a distribuição de carga de acessos aos sistemas, tanto em ambiente interno quanto externo, tanto no ambiente das aplicações modernas quanto das aplicações legadas, nos diversos servidores de aplicação disponíveis na infraestrutura da Justiça Eleitoral, garantindo os requisitos necessários de segurança, desempenho e disponibilidade, principalmente, para sistemas críticos.

1.11. Trata-se a ampliação ou substituição da solução implantada? ( ) SIM (X) NÃO

2. ESPECIFICAÇÃO DOS REQUISITOS

2.1 Requisitos da Contratação

O presente estudo objetiva a contratação de Solução de Segurança da Informação – Controle e Proteção de Aplicação, visando aumentar a disponibilidade, confidencialidade e integridade dos Sistemas e Aplicativos do Tribunal Regional Eleitoral do Pará

2.2 Requisitos Gerais da Solução de TIC

- A solução poderá ser fornecida na modalidade de appliance físico ou virtual, dependendo da demanda do regional partícipe da Ata RP.
- A solução de Web Application Firewall deve ser fornecida e instalada, garantindo pleno funcionamento, com todas as licenças, recursos, funcionalidades e complementos, conforme definido no Termo de Referência ou Edital, sem a necessidade de contratação de serviço(s) adicional(is).
- Cada pacote de software ofertado deve ser instalado em sua última versão estável e estar coberto por contrato de suporte e atualização de versão pelo(s) fabricante(s) durante a vigência da garantia de 60 (sessenta) meses.
- Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a Contratada a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam.
- A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.
- A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise).
- No momento da apresentação das propostas, todos os componentes constantes da Solução deverão possuir EOL (End-of-life) e EOS (End-of-support) não definidos ou anunciados.

2.3. Requisitos de capacitação

- Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares em produção, bem como planejar mudanças de configuração no ambiente.

  a) O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas.
  b) Serão aceitos apenas treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE.
  c) A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes.
  d) Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia.
  e) O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução.

- As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA.
- O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante.
- A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertados atendem os requisitos indicados no item (e) anterior.
- O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário.
- O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dos equipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada.
- É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do contratado para todos os fins.
- O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato.
- A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português.
- O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês.
- O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos.
  - No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.
  - Após a conclusão da capacitação, o ambiente EAD deverá permanecer disponível ao acesso do aluno por um prazo mínimo de 12(doze) meses, sob demanda do CONTRANTE.
- A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o

certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.

- A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor.
- A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência.

a) No Formulário, será utilizada escala de até 4 (quatro) pontos para cada quesito do formulário. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso.
b) O resultado da Avaliação de Instrutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como "proveitoso" para no mínimo 04(quatro) dos 07(sete) itens avaliados;
c) Caso o resultado da Avaliação de Instrutor seja considerado "não proveitoso", o treinamento fornecido será considerado não aceito;
d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE;
e) Na hipótese de o resultado do segundo treinamento ser "não proveitoso", o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

2.4. Requisitos legais

- A CONTRATADA deve observar o cumprimento de todas as leis e normas aplicáveis ao OBJETO, em especial atenção àquelas relacionadas ao pagamento das obrigações empresariais relacionadas à encargos fiscais, trabalhistas e previdenciários.
- Outras Referências:
  - Portaria n°18456/2019, estabelece as diretrizes para a Gestão de Ativos de Tecnologia da Informação e Comunicações e institui o processo de gestão de configuração e ativos de TIC no âmbito do TRIBUNAL REGIONAL ELEITORAL DO PARÁ – TRE-PA;
  - Resolução CNJ N° 182/2013, dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ);
  - Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);
  - Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);
  - LGPD – Lei Geral de Proteção de Dados (Lei n° 13.709/2018) e Marco Civil da Internet Lei no 12.965/2014);
  - Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;
  - Lei 8.666/1993, regulamenta o art. 37, inciso XXI, da Constituição Federal, institui normas para licitações e contratos da Administração Pública e dá outras providências.
  - Instrução Normativa Nº 1, de 4 de abril de 2019. Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;
  - Decreto 9.488/2018, altera o Decreto nº 7.892, de 23 de janeiro de 2013, que regulamenta o Sistema de Registro de Preços previsto no art. 15 da Lei nº 8.666, de 21 de junho de 1993, e o Decreto nº 7.579, de 11 de outubro de 2011, que dispõe sobre o Sistema de Administração dos Recursos de Tecnologia da Informação - SISP, do Poder Executivo federal.

2.5. Requisitos de manutenção

- A CONTRATADA deverá fornecer garantia técnica de pelo menos 60 (sessenta) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação;
- Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para o CONTRATANTE, obrigando-se a Contratada a manter os equipamentos e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam;
- A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software;
- Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 48 (quarenta e oito) horas a partir de notificação do CONTRATANTE;
- A Contratada deverá apresentar no protocolo do CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários para o registro de chamados técnicos na Central de Atendimento da Contratada, tais como, e-mail, números de telefone e fax, etc;
- Suporte Técnico durante o período de Garantia Técnica:
  - Durante o período de garantia técnica de 60 (sessenta) meses, a partir do recebimento definitivo da instalação, a Contratada deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção;
  - A Contratada deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica do CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços contratados;
  - A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação do CONTRATANTE;
- A contratada deverá entregar no protocolo do CONTRATANTE, mensalmente, até o 5° (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações:
  - Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico do CONTRATANTE que solicitou e validou o chamado; identificação do técnico da

Contratada responsável pela execução do chamado, bem como outras informações pertinentes;
    - Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;
    - O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido;
    - O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A Contratada deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.
- A Contratada deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos equipamentos da solução.
- A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à Contratada orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos equipamentos, desde que tal iniciativa não implique em danos físicos e lógicos aos equipamentos, sem que isto possa ser usado como pretexto pela Contratada para se desobrigar do suporte da solução.
- A Contratada deverá garantir pleno funcionamento dos equipamentos e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução contratada.
- A Contratada deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos equipamentos e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local por todo o período da garantia técnica.
- A Contratada deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos equipamentos nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;
- O serviço de garantia técnica deverá permitir o acesso do CONTRATANTE à base de dados de conhecimento do fabricante dos equipamentos, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos equipamentos.
- As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta forma forem solicitadas.
- Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a Contratada deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento.
- A Contratada deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

2.6. Requisitos temporais

Deverá ser realizada após a assinatura do Contrato, uma reunião de alinhamento remota, com o objetivo de alinhar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas acerca do objeto, conforme agendamento efetuado pelo Gestor do Contrato, bem como:

- Apresentar a relação do pessoal técnico especializado, adequado e disponível para a execução do objeto deste Estudo, bem como a qualificação de cada um dos membros da equipe técnica.
- Apresentar a declaração de disponibilidade, assinada por cada integrante da equipe técnica mencionada na alínea anterior, bem como o Termo de Confidencialidade da Informação.
- Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato.
- Apresentar a logística para realização do treinamento da Solução adquirida.
- Os profissionais indicados pela Contratada deverão efetivamente implantar e configurar a Solução objeto deste Estudo, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo órgão.
- O prazo para a entrega, instalação e configuração da solução será de até 60 (sessenta) dias consecutivos, contados a partir do primeiro dia útil após a confirmação de recebimento da Ordem de Fornecimento emitida pela Fiscalização do Contrato.
- O prazo de implantação da solução será de até 30(trinta) dias a partir do recebimento do objeto.

2.7. Requisitos de segurança da informação

- A Contratada deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da Contratante.
- A empresa contratada deverá respeitar as diretrizes constantes da **Política de Segurança da Informação do da Justiça Eleitoral** (Resolução TSE No 23.501/2016), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Pará, e de outros partícipes desta contratação, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa;
- O Tribunal Regional Eleitoral do Pará terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação;
- Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).
- O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver

acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

2.8. Requisitos de Arquitetura Tecnológica

- O CONTRATANTE fornecerá à CONTRATADA:

  a) Acesso físico às dependências relacionadas à prestação dos serviços;

  b) Acesso lógico e os respectivos privilégios adequados nos sistemas, aplicações e ferramentas necessárias a perfeita execução dos serviços, exclusivamente para os profissionais diretamente envolvidos em sua execução; e

  c) Acesso às soluções de hardware e software de sua propriedade necessárias à execução das atividades contratadas, não desobrigando a CONTRATADA de fornecer eventuais soluções de softwares especificadas na contratação (quando for o caso).

  d) O ambiente virtualizado, de acordo com os requisitos mínimos, para instalação completa da solução de segurança da informação para sistemas críticos apresentadas neste documento.

- Caberá à CONTRATADA toda providência junto ao fabricante/fornecedor e/ou detentor da propriedade intelectual da solução tecnológica quanto à emissão de licenças e termos de garantia relacionados à solução contratada que pertencerão exclusivamente ao CONTRATATANTE.
- À CONTRATADA caberá fornecer todos os demais recursos e condições técnicas necessárias à execução dos serviços, incluindo ferramentas específicas, materiais de apoio, materiais de identificação, equipamentos de proteção individual, etc.

2.9. Requisitos de Projeto e de Implementação

- Os serviços de implantação serão executados pela CONTRATADA e deverão ser estruturados conforme as fases a seguir.

  I - Fase de abertura
  a.)Validar e Homologar escopo do projeto;
  b) Validar objetivos e premissas do projeto;
  c) Validar riscos e restrições do projeto;
  d) Identificar e validar os requisitos do projeto;
  e) Efetuar o levantamento de informações sobre o ambiente atual, em complementação ao conjunto de informações apresentado nesta especificação técnica;
  f) Efetuar o gerenciamento de mudanças, contemplando análise de riscos de implementação do sistema;
  g) Apresentar o estudo dos riscos envolvidos na migração para o novo sistema a ser implantado.

  II - Fase de planejamento
  a) Elaborar plano de projeto;
  b) Definir as pessoas envolvidas por parte da CONTRATANTE no projeto;
  c) Reunir as equipes da CONTRATADA e CONTRATANTE;
  d) Definir os parâmetros de configuração básicos e avançados a serem implementados;
  e) Apresentar o Mapa de rede contendo a topologia a ser implementada;
  f) Apresentação do cronograma do projeto com os prazos e responsabilidades;
  g) Verificar os pré-requisitos do projeto;
  h) Apresentar plano do projeto para a homologação por parte da CONTRATANTE.

  III - Fase de execução

  O serviço de instalação consiste na colocação do(s) equipamento(s) em pleno funcionamento, em conformidade com o disposto neste Estudo, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da CONTRATANTE e deve contemplar, no mínimo, o seguinte:
  a) Deverão ser realizados por conta da contratada o armazenamento, a embalagem, o transporte, a entrega e a instalação de todo e qualquer item do objeto do edital, de tal maneira que a contratada será responsável pela remessa de todos os equipamentos para o(s) endereços informados no Edital, nos quais a solução de segurança será efetivamente implantada.
  b) A CONTRATADA deverá efetuar instalação e configuração realizada de acordo com as recomendações do fabricante (recommended settings);
  c) A CONTRATADA deverá efetuar a instalação do appliance virtual ou físico (conforme item solicitado) na infraestrutura indicada pelo CONTRATANTE, onde a configuração realizada deverá estar em conformidade com as recomendações do fabricante (recommended settings);
  d) Conexão e configuração de todos os equipamentos e/ou componentes da solução da rede do CONTRATANTE, inclusive configuração de VLANs e interfaces virtuais, se for o caso;
  e) Atualização de softwares, firmwares e drivers que compõem a solução;
  f) A CONTRATADA deverá fornecer, quando for o caso, todos os equipamentos, componentes, acessórios e cabos de conexão para interligar fisicamente todos os componentes da solução entregue;
  g) Aplicação das licenças necessárias à solução entregue;
  h) Testes da solução, incluindo testes de failover;
  i) Documentação do ambiente configurado e instalado.

2.10. Requisitos de Implantação

- A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para a contratante, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dos equipamentos poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade ou que venham a requerer a parada dos equipamentos deverão ser executadas fora do horário de expediente, inclusive em

feriados ou finais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE.
- Atividades associadas à implantação com a necessidade de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE.
- Para todos os efeitos, a conclusão dos serviços de instalação e configuração será atestada pela entrega do sistema em pleno funcionamento, incluindo documentação "As Built", contendo planejamento, relatório de instalação, configuração adotada, testes realizados e seus resultados, de acordo com as especificações do(s) fabricante(s) e demais condições estabelecidas para a contratação.

2.11. Requisitos sociais, ambientais e culturais

- *A documentação e os manuais da solução deverão, preferencialmente, ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).*
- *O licenciamento e o suporte devem ser prestados preferencialmente no idioma português do Brasil.*
- *Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.*
- *Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.*

2.12. Requisitos de experiência profissional

- *A implantação deve ser realizada por profissionais certificados, que possuam certificação do fabricante da solução adquirida ou pelo próprio fabricante, que lhes confiram as competências necessárias para a realização dos respectivos serviços.*
- *Para esta solução é necessária a capacitação do corpo técnico e implementação com acompanhamento de um profissional especializado na solução e/ou pelo próprio fabricante, por se tratar de uma solução complexa.*
- *A proponente deverá possuir pelo menos 1 (um) profissional capacitado com certificação, e deverá apresentar certificado técnico da solução durante a fase de habilitação.*
- *Os profissionais que inicialmente manterão relacionamento direto com o CONTRATANTE deverão ser apresentados após assinatura do CONTRATO na REUNIÃO INICIAL, ocasião em que deverão ser entregues as comprovações dos perfis exigidos. A apresentação de novos profissionais durante a execução do CONTRATO, incluindo a entrega das comprovações dos perfis à equipe de fiscalização do CONTRATO, deverá ser feita previamente ao início da atuação destes.*

3. ESTIMATIVA DA DEMANDA PREVISTA E A QUANTIDADE DE BENS E SERVIÇOS (Art. 14, IV, d)

O art. 21 da Resolução 370/2021 (Estratégia Nacional de Tecnologia da Informação e Manutenção do Poder Judiciário - ENTIC-JUD), que estabelece a constituição e manutenção de estruturas organizacionais adequadas e compatíveis com a demanda de TIC, cita expressamente a disponibilidade como parte do macroprocesso de infraestrutura e serviços, sendo este macroprocesso considerado como requisito mínimo para atendimento das demandas de TIC.

Deste modo, o objeto da contratação tem por objetivo assegurar a proteção de aplicações WEB e informações sensíveis armazenadas nos servidores em produção por meio solução de Web Appliaction Firewall. Para tanto, devido a necessidade da contratação, as quantidades abaixo foram estimadas durante a realização do Estudo Técnico Preliminar para compor o projeto em sua totalidade, considerando a demanda específica da solução; além da necessidade de contratação de serviços de implantação, treinamento, e garantia técnica:

DEMANDA EXISTE	QTDE	DESCRIÇÃO DA SOLUÇÃO DE TI A SER CONTRATADA	JUSTIFICATIVAS
PROTEÇÃO DE APLICAÇÕES WEB PUBLICADAS NA INTERNET/INTRANET ,HOSPEDADAS NO DATA CENTER DO	2	CLUSTER/SOLUÇÃO DE PROCEÇÃO CAMADA 7 PARA APLICAÇÕES WEB, FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL.	Cluster de proteção (2 appliances) das aplicações WEB hospedadas no ambiente de produção (Data Center) do Tribunal, visando mitigar os riscos de ataque cibernético, com Garantia e suporte técnico do fabricante, período de 60(sessenta) meses, necessárias à manutenção da disponibilidade da solução. ** O fornecedor*
		CLUSTER/SOLUÇÃO	

TRIBUNAL	2	DE PROCEÇAO CAMADA 7 PARA APLICAÇÕES WEB, FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO.	*deverá prover a solução na modalidade de apppliance Físico e Virtual, em razão da necessidade de cada Regional partícipe da Ata RP.* *** Deverão ser fornecidas 2(duas) unidades da solução, em cada modalidade, para configuração do cluster, em razão da redundância do serviço.*
LICENCIAMENTO EXPANSÃO DE CAPACIDADE	2	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	Capacidade adicional para solução em Firewall de Aplicações WEB, visando a expansão de capacidade da Taxa de transferência (throughput) da solução.
IMPLANTAÇÃO / REPASSE DE CONHECIMENTO HANDS-ON	1	IMPLANTAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução.
	6	TREINAMENTO ESPECIALIZADO	Capacitação da equipe técnica (até 6 servidores) para administração da solução, por meio de treinamento.

Tabela 1 - Levantamento da demanda e quantidades e solução/serviço de TI a ser contratado.

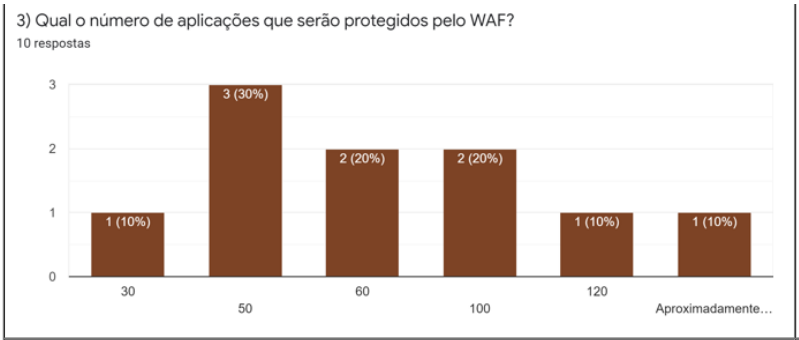
3.1. REQUISITOS E CARACTERÍSTICAS DOS REGIONAIS PARTÍCIPES DA ATA RP

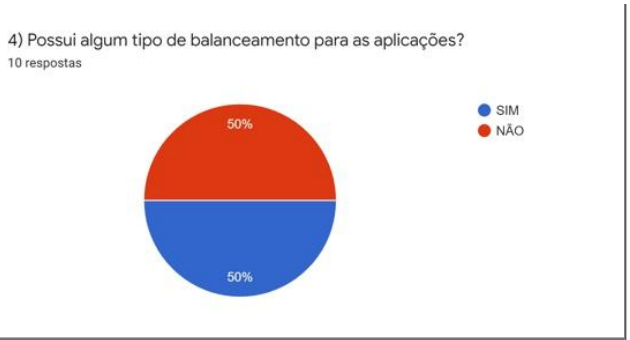
Através de formulário de pesquisa, foi efetuado o levantamento de algumas informações relacionadas aos requisitos de ambiente de cada Tribunal. Além disso, foram incluídos questionamentos sobre a preferência de cada TRE quanto ao fornecimento da solução (Appliance Físico ou Appliance Virtual).

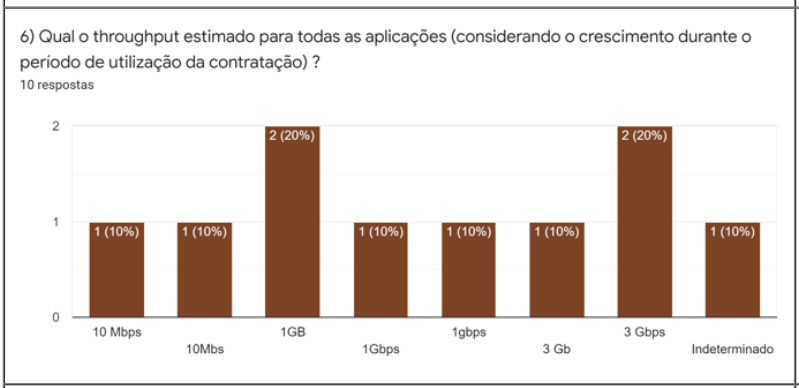
As respostas indicam características similares entre os ambientes dos TREs que devem ser protegidos pela solução, como topologia, utilização de solução de microserviços (Docker/Kubernet, outros), além de apontar para algumas necessidades, que devem ser contempladas pela contratação, como, por exemplo:

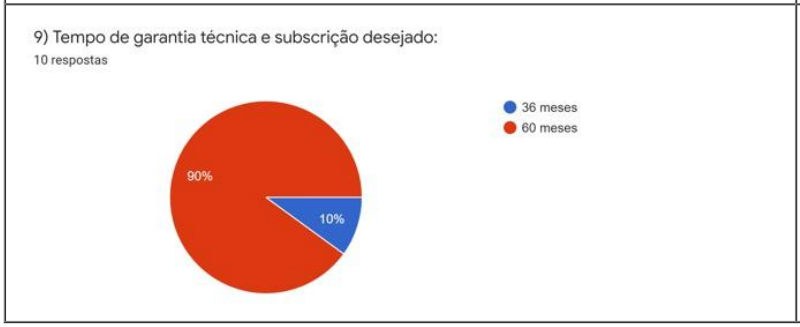
- o prazo de garantia;
- a quantidade de aplicações que a solução deve proteger;
- o throughput estimado para todas as aplicações (considerando o crescimento durante o período de utilização da contratação);
- a preferência para entrega da solução: Appliance Físico ou Appliance Virtual;
- se o ambiente do TRE possui suporte para rede 10Gb.

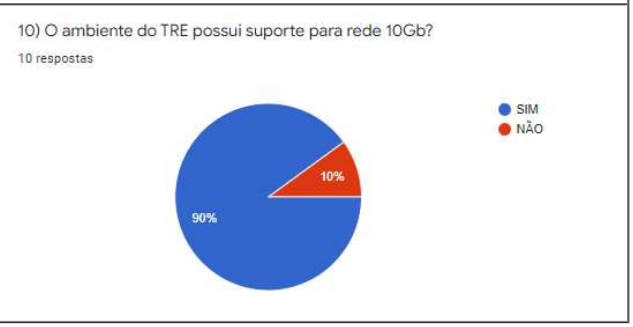
O quadro a seguir exibe algumas respostas que consideramos pertinentes figurar neste Estudo Preliminar, encaminhadas pelos seguintes TREs: TRE-RJ, TRE-RO, TRE-SC, TRE-TO, TRE-AM, TRE-ES, TRE-PA, TRE-PB, TRE-PR e TRE-PE.











Neste contexto, em razão da similaridade das topologias de rede, sistemas e aplicações em ambientes de produção (SHRG WEB, ASIWEB, SEI, Intranet, etc) existentes nos Tribunais, entendemos que a solução proposta por este Regional apresenta compatibilidade com a demanda existente, em outros TREs que desejam participar da contratação conjunta.

4. ESTRATÉGIA DA CONTRATAÇÃO DO OBJETO

( ) Pregão Eletrônico - Sistema de Registro de Preços

( ) Adesão a Ata de Registro de Preços

(X) IRP (Intenção de Registro de Preços) - Contratação conjunta

( ) Contratação Direta (Art. 24 e incisos da Lei 8666/93)

( ) Inexigibilidade (Art. 25 da Lei 8666/93)

4.1. Necessidade de apresentação da fundamentação com base nos Art. 3º e Art. 22. do Decreto nº 7.892/2013, o que concerne na justificativa para adoção de ARP e autorização de carona para órgão não partícipe:

a) Quanto à justificativa de adoção da ARP:

Inciso IV - quando, pela natureza do objeto, não for possível definir previamente o quantitativo a ser demandado pela Administração.

- Uma vez que não há como prever, no prazo de 12(doze) meses de vigência da ata, a demanda ou quantidade de itens que podem ser demandados pelos Tribunais partícipes da contratação conjunta, faz-se necessário a utilização de registro de preços, conforme incisos II e III, Art. 3º e Art. 22. do Decreto nº 7.892/2013.

  II - quando for conveniente a aquisição de bens com previsão de entregas parceladas ou contratação de serviços remunerados por unidade de medida ou em regime de tarefa;

  III - quando for conveniente a aquisição de bens ou a contratação de serviços para atendimento a mais de um órgão ou entidade, ou a programas de governo;

b) Quanto à autorização de carona para órgãos não partícipes:

- Por não haver excepcionalidade, conforme orientações dos Acórdãos TCU nº 757/2015- Plenário e 2037/2019 – Plenário, o objeto da ARP não possibilitará adesões de outros órgãos da Administração Pública.

4.2 Forma de Parcelamento e Adjudicação do Objeto

4.2.1. Natureza do Objeto

- O objeto associado à contratação é considerado comum, pois apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio

de especificações usuais de mercado.

4.2.2. Parcelamento do Objeto

- Como se trata de pregão tradicional, a ordem de fornecimento derivada do processo de licitação deverá ser realizada por meio de pedido integral da solução.

4.2.3. Adjudicação do Objeto

- Adjudicação por Lote devido a necessidade de compatibilidade e vínculos diretos entre seus itens componentes.

4.2.4. Modalidade e Tipo de Licitação

- Pregão Eletrônico do Tipo Menor Preço.

4.2.5. Justificativa para o agrupamento de itens

- O agrupamento dos itens do objeto do presente Instrumento em lote, tem por objetivo a padronização da contratação uma vez que os itens agrupados possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores traz ineficiência e custo na gestão e fiscalização da contratação.
- Além disso, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou provoca a perda de economia de escala. Neste sentido, justifica-se o agrupamento em lote, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.
- Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um fornecedor e melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Estudo Preliminar.
- Isto posto, o agrupamento através de um único lote visa a garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existentes no Tribunal com os serviços prestados com a contratação.

5. Indicação da Necessidade de Adequação Ambiental

TIPO DE NECESSIDADE	RESPONSÁVEL	DESCRIÇÃO
Infraestrutura tecnológica	CONTRATADA	A instalação da solução de segurança utilizará a rede lógica corporativa do Tribunal. A solução deverá ser instalada no(s) Data Center(s) do Tribunal.
Mudança ou Configuração	CONTRATADA	Os serviços de instalação e configuração deverão se basear nas melhores práticas estabelecidas pelo respectivo fabricante em seus manuais de instalação e configuração ou artigos técnicos
Infraestrutura elétrica	CONTRATANTE	O dimensionamento e disponibilização de energia elétrica para o funcionamento da solução, quando for o caso, ficará por conta do Tribunal.
Logística de implantação	N/A	Após a entrega dos equipamentos pela CONTRATADA, recebimento e aceite pela fiscalização do Contrato, estes deverão ser configurados e instalados, também pela CONTRATADA, com supervisão da equipe técnica do CONTRATANTE. A critério do CONTRATANTE, os serviços poderão ser executados fora do horário comercial e/ou em finais de semana ou feriados sem custo adicional para o contratante, visando minimizar os transtornos aos usuários devido a uma eventual indisponibilidade dos serviços. Por conseguinte, as atividades que não tenham impacto de indisponibilidade ou que não venham a requerer a parada dos equipamentos poderão ser executadas em horário comercial. Para as atividades que tenham impacto de disponibilidade ou que venham a requerer a parada dos equipamentos deverão ser executadas fora do horário de expediente, inclusive em feriados ou finais de semana, de acordo com o estabelecido entre a CONTRATADA e o CONTRATANTE. Atividades associadas à implantação com a necessidade de interrupção de serviços em produção, deverão ocorrer fora do expediente normal do Tribunal e estarão sujeitas ao planejamento e aprovação prévia da equipe técnica da CONTRATANTE.
Espaço físico	CONTRATANTE	Será disponibilizado espaço físico no rack dos Data Centers para a instalação dos equipamentos da solução a ser

		contratada.
Mobiliário	N/A	Não será necessário mobiliário.
Impacto ambiental	N/A	Não haverá impacto ambiental na implantação da solução objeto deste Estudo.

Tabela 2 - Indicação da Necessidade de Adequação Ambiental

***

ANEXO A

ANÁLISE DE SOLUÇÕES DISPONÍVEIS NO MERCADO DE TIC

I - PESQUISA DE SOLUÇÕES DISPONÍVEIS NO MERCADO E RESPECTIVOS FORNECEDORES (Art. 14, I, a)

A presente contratação visa à aquisição de solução de segurança e proteção de aplicações - WAF (Web Application Firewall), com a finalidade de aumentar a segurança dos sistemas, aplicações e processos deste Egrégio Tribunal. Cumpre destacar que, atualmente, o poder judiciário não possui ferramenta específica de proteção supramencionada e, conforme detalhamento do potencial da solução, busca a aquisição da plataforma que apresentar a proposta mais vantajosa, em qualidade, técnica e preço.

Objeto associado à contratação é considerado comum, pois apresenta padrões de desempenho e qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado. Sendo uma solução comum de mercado, é notório que existem diversos fabricantes que oferecem soluções de WAF (Web Application Firewall) de diferentes portes/configuração (incluindo appliance físico ou virtual), que suportam diversas funções como Load Balancing (LB) e DDoS Mitigation, com diferenciados valores. Dentre os fabricantes mais comuns em licitações, constam os seguintes: (1) VMWare, Pulse Secure e Huawei, considerando a abordagem de appliance virtual; (2) F5, A10, Citrix, Radware, Imperva, considerando a abordagem tradicional ("On-Premise"), que também entregam a solução na modalidade de appliance virtual.

De outro lado, também existem soluções que são fornecidas em infraestrutura de Cloud (nuvem), que não serão consideradas na análise desta contratação, uma vez que optou-se por contratação de infraestrutura *on-premise*.

Sendo inviável avaliar todas as opções disponíveis, recorreu-se a duas fontes de pesquisa reconhecidos no mercado de Tecnologia. a Forrester Wave e Gartner Group.

O Forrester Wave, é referência na área de consultoria em soluções de Tecnologia da Informação e foi utilizada para delimitar as melhores opções a serem consideradas na análise de soluções disponíveis. O Forrester Wave possui um "quadrante", onde são utilizados diversos critérios para avaliar a qualidade das soluções. Como esta Justiça Especializada preza isonomia e qualidade técnica das soluções para compor sua infraestrutura tecnológica, as soluções consideradas na análise foram as que se enquadram nos quadrantes "Leaders" e "Strong Performers" do quadrante mais recente, publicado em 2021. Os fabricantes localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas.

FORRESTER® RESEARCH

THE FORRESTER WAVE™

Web Application Firewalls

Q1 2020

157258 Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Ao que podemos verificar no quadrante do Forrester Wave, existem diversos fabricantes líderes em soluções de WAF, como, por exemplo, Imperva Cloud WAF, Radware, F5, Barracuda e Radware.

Além da Forrester, outra empresa que promove pesquisas de mercado sobre tecnologias é o Gartner Group. O Gartner Group é uma das principais empresas mundiais especializadas pesquisa e consultoria em tecnologia da informação. Sua missão consiste em gerar informações, métricas e análises a respeito de tecnologia para que seus clientes tomem decisões estratégicas, fundamentadas em informações, artigos e publicações que revelam as principais tendências do mercado de tecnologia.

A Gartner publica estudos regularmente, chamados de **Quadrantes Mágicos**, que avaliam provedores de tecnologia nas mais diversas áreas e aplicações. O estudo apresenta uma visão de alto nível dos principais provedores para um determinado mercado de tecnologia, mostrando como as soluções estão posicionadas para atender a estratégia das organizações a longo prazo. O Gartner aplica um conjunto uniforme de critérios de avaliação aos competidores e os posiciona relativamente em um gráfico.

De acordo com o Gartner, até 2023, mais de 30% dos aplicativos da Web voltados para o público serão protegidos por aplicativos da Web em nuvem e serviços de proteção de API (WAAP) que combinam proteção distribuída de negação de serviço (DDoS), mitigação de bot, proteção de API e WAFs.

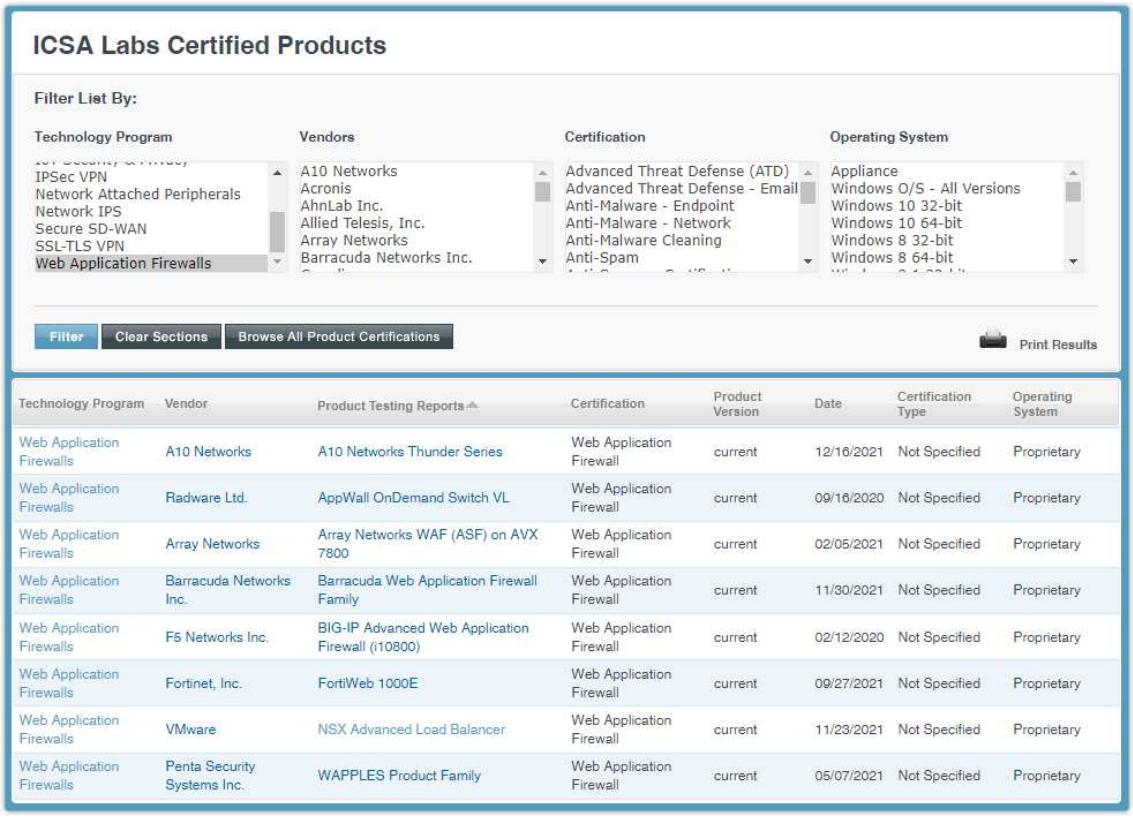
As soluções consideradas na análise foram as que se enquadram nos quadrantes “Leaders” e “Challenders” para o mercado de WAF, segundo a publicação mais recente, conforme a seguir

Source: Gartner (October 2020)

Conforme o **Quadrantes Mágico** para soluções WAF, Imperva e Akamai figuram como Leaders, enquanto outras soluções como Cloudflare, F5, Barracuda e Fortinet aparecem como Challenders.

Outra fonte de pesquisas, bastante conhecida, sobre os fornecedores do mercado de soluções de Segurança da Informação é ICSA Labs. O ICSA Labs é uma divisão independente da Verizon, que fornece informações confiáveis e independente de produtos de terceiros para usuários finais e empresas desde 1989. O ICSA Labs fornece testes e certificação de terceiros para produtos de segurança de TI. ICSA Labs utiliza testes objetivos e critérios de certificação para medir a conformidade, confiabilidade e desempenho do produto para a maioria dos principais fornecedores de tecnologia do mundo.

O ICSA Labs disponibiliza na URL https://www.icsalabs.com/products?tid[]=4227 uma pesquisa para fornecedores de **Web Application Firewalls**, conforme demonstrado a seguir:



ICSA Labs Certified Products

Filter List By:

Technology Program: IPSec VPN; Network Attached Peripherals; Network IPS; Secure SD-WAN; SSL-TLS VPN; Web Application Firewalls

Vendors: A10 Networks; Acronis; AhnLab Inc.; Allied Telesis, Inc.; Array Networks; Barracuda Networks Inc.; Anti-Spam

Certification: Advanced Threat Defense (ATD); Advanced Threat Defense - Email; Anti-Malware - Endpoint; Anti-Malware - Network; Anti-Malware Cleaning

Operating System: Appliance; Windows O/S - All Versions; Windows 10 32-bit; Windows 10 64-bit; Windows 8 32-bit; Windows 8 64-bit

Filter | Clear Sections | Browse All Product Certifications | Print Results

Technology Program	Vendor	Product Testing Reports	Certification	Product Version	Date	Certification Type	Operating System
Web Application Firewalls	A10 Networks	A10 Networks Thunder Series	Web Application Firewall	current	12/16/2021	Not Specified	Proprietary
Web Application Firewalls	Radware Ltd.	AppWall OnDemand Switch VL	Web Application Firewall	current	09/16/2020	Not Specified	Proprietary
Web Application Firewalls	Array Networks	Array Networks WAF (ASF) on AVX 7800	Web Application Firewall	current	02/05/2021	Not Specified	Proprietary
Web Application Firewalls	Barracuda Networks Inc.	Barracuda Web Application Firewall Family	Web Application Firewall	current	11/30/2021	Not Specified	Proprietary
Web Application Firewalls	F5 Networks Inc.	BIG-IP Advanced Web Application Firewall (i10800)	Web Application Firewall	current	02/12/2020	Not Specified	Proprietary
Web Application Firewalls	Fortinet, Inc.	FortiWeb 1000E	Web Application Firewall	current	09/27/2021	Not Specified	Proprietary
Web Application Firewalls	VMware	NSX Advanced Load Balancer	Web Application Firewall	current	11/23/2021	Not Specified	Proprietary
Web Application Firewalls	Penta Security Systems Inc.	WAPPLES Product Family	Web Application Firewall	current	05/07/2021	Not Specified	Proprietary

Por fim, da mesma forma que constatamos no Forrester Wave o Gartner Group a pesquisa no ICSA Labs listou basicamente os mesmos fabricantes para a solução em tela, demonstrando que mercado de soluções de WAF possui diversos fornecedores, o que remete a possibilidade do aumento da concorrência no certame licitatório.

II - SOLUÇÕES BASEADAS EM SOFTWARE LIVRE E/OU OPEN SOURCE

Além das soluções de mercado, existem também soluções WAF em Software Livres e Open Source. Dentre eles, destaca-se o ModSecurity (https://www.modsecurity.org/) da TrustWave, que é um dos firewalls de aplicativos da Web mais populares e suporta Apache HTTP, Microsoft IIS e Nginx. O ModSecurity possui uma linguagem de programação robusta baseada em eventos que fornece proteção contra uma série de ataques contra aplicativos da Web e atua principalmente no monitoramento do protocolo HTTP, realizando registro e análise em tempo real. Entretanto, a TrustWave anunciou o fim da vida útil (EOL) do suporte para o ModSecurity a partir de 1º de julho de 2024, informando ainda que a manutenção do código ModSecurity seria entregue de volta à comunidade de código aberto. Outras alternativas são o Ironbee e Zorp, entretanto as soluções propostas, baseadas em software livre e open source, são bastante limitadas se comparadas com os recursos disponíveis em softwares comerciais.

Entretanto, conforme demonstrado no item "3. ESTIMATIVA DA DEMANDA", a solução de segurança WAF requer outros serviços, como treinamentos, suporte especializado para implantação e operação. Além disso, apesar da possibilidade da composição da solução ser factível para Software Livre, as tarefas para integração, implantação e manutenção da solução sobre a equipe de Segurança demandariam elevado tempo até que seja alcançado um nível de proteção minimamente adequado, sendo inclusive inevitável a necessidade de integração de diferentes softwares e soluções, na maioria das vezes, sem a possibilidade de suporte especializado externo. Por contar com um quantitativo de equipe reduzida para a administração da segurança da informação, os tribunais não poderiam contar com o auxílio de contratação de empresas especializadas para solucionar problemas técnicos que poderiam surgir.

Neste cenário, a solução poderia tornar-se limitada ou insuficiente para resolução de ataques emergentes e, um eventual incidente, a correlação e análise detalhada das informações contidas nos softwares de diferentes fontes poderia levar horas ou dias, comprometendo a investigação dos eventos, a preservação de evidências e a disponibilidade e segurança da rede.

Portanto, manter e gerenciar uma solução totalmente baseada WAF baseada em softwares livres, para o caso em tela, acarreta custo operacional elevado, bem como alto custo de manutenção do ambiente de missão crítica. Dificulta, ainda, o estabelecimento de processos de gestão da segurança da informação, inviabilizando a especialização da equipe para operação dos sistemas e suas funcionalidades, visto que serão necessários estudos internos e diversos treinamentos para softwares distintos que nem sempre irão garantir sua interoperabilidade.

III. IDENTIFICAÇÃO DAS SOLUÇÕES (Art. 14, II)

ID	DESCRIÇÃO DA SOLUÇÃO (OU CENÁRIO)
1	Web Application Firewall - WAF baseado em Solução de Mercado
2	Web Application Firewall - WAF baseado em Software Livre

ALTERNATIVA	Solução	Sim	Não	Não se Aplica

A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2		X	
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1		X	
	Solução 2	X		
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X

IV. DISPONIBILIDADE DE SOLUÇÃO SIMILAR EM OUTRO ÓRGÃO OU ENTIDADE DA ADMINISTRAÇÃO PÚBLICA (Art. 14, I, b)

Contratações similares, dentre os quais foram adquiridos soluções WAF dos fornecedores mencionados, já estão sendo adotadas em diversos órgãos da Administração Pública, possivelmente devido ao disposto no DECRETO Nº 10.222, DE 5 DE FEVEREIRO DE 2020, que aprova a Estratégia Nacional de Segurança Cibernética do Executivo Federal; assim como, em razão da Resolução CNJ 396/2021 que Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Relacionamos abaixo alguns casos:

#	ÓRGÃO PÚBLICO	OBJETO	INSTRUMENTO (Contrato, PE, Ata RP)
1	EMPRESA DE TECNOLOGIA E INFORMAÇÕES DA PREVIDÊNCIA - DATAPREV	Registro de preços para aquisição de até 58 (cinquenta e oito) equipamentos (appliance) de controle de entrega de aplicação (Application Delivery Controller - ADC), Balanceador Global (Balanceamento de sites) e Firewall de Aplicação Web (WAF – Web Application Firewall) de hardware e software destinados ao Datacenter, com garantia de 60 (sessenta) meses.	PREGÃO ELETRÔNICO No 2019/ 01355
2	TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO	Solução de Balanceadores de Carga de aplicação para a implantação nos perímetros de usuário e de DataCenter, de modo a permitir, entre outras funções, o balanceamento de carga entre as aplicações, além de fornecer mecanismos de segurança mais específicos, incluindo, equipamentos físicos, solução de gerenciamento da solução, serviço de implantação/migração, treinamento, suporte técnico, suporte técnico especializado (sob demanda), pelo prazo de 51 (cinquenta e um) meses, conforme Anexo IA (Complementação ao Termo de Referência) e, conforme especificado no termo de referência (ANEXOI).	PREGÃO ELETRÔNICO N° 0046/2021
3	TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO	Contratação de empresa especializada no fornecimento, instalação e configuração de sistema de balanceamento de carga de aplicações com firewall de aplicação integrado, incluindo testes	PREGÃO

3	ESTADO DO RIO GRANDE DO SUL	operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, bem como os serviços de migração, treinamento, garantia e de suporte técnico.	ELETRÔNICO Nº 198/2019
4	TRIBUNAL REGIONAL FEDERAL DA PRIMEIRA REGIÃO	Registro de preços para eventual aquisição de Solução de Segurança da Informação - Controle de Aplicação com assistência técnica da garantia de 60 (sessenta) meses, compreendendo os serviços de Implantação da Solução, Operação Assistida, Treinamentos e Consultoria Técnica.	PREGÃO ELETRÔNICO SRP N° 41/2016
5	TRIBUNAL DE CONTAS DO ESTADO DO AMAPÁ	Contratação de empresa especializada para o fornecimento de Solução integrada de segurança, composta por um cluster de Gerenciamento Unificado de Ameaças (Firewall UTM) e seu Gerenciamento de Logs e Relatórios de Segurança; Solução em Firewall de Aplicações WEB (WAF - Web Application Firewall).	PREGÃO ELETRÔNICO Nº 01/2021

**A análise de projetos similares realizados anteriormente pelo TRE-PA.*

CONTRATAÇÕES SIMILARES REALIZADAS ANTERIORMENTE PELO TRIBUNAL		
OBJETO	**INSTRUMENTO (Contrato, PE, Ata RP)**	**QTDE**
Não existem contratações anteriores		

AVALIAÇÃO DAS ALTERNATIVAS DE SOLUÇÃO

REQUISITOS DESEJÁVEIS		**SOLUÇÃO 1**		**SOLUÇÃO 2**	
Descrição	Peso	Avaliação	Nota	Avaliação	Nota
Eficiência	8	3	24	1	8
Eficácia	8	3	24	2	16
Economicidade	5	2	10	1	5
Dependência de outras soluções	5	1	5	3	15
Segurança	10	3	30	2	20
Suporte	10	3	30	0	0
Treinamento	10	3	30	0	0
Nota Final		153		64	

0 - Não atende; 1 – Atende precariamente; 2 – Atende parcialmente; 3 – Atende completamente

V - ORÇAMENTO ESTIMADO (Art. 14, II, g)

FONTE 1:

A tabela abaixo diz respeito aos valores dos itens 1, 2 e 3 referentes Pregão Eletrônico 0032/2021, realizado pelo TRIBUNAL REGIONAL ELEITORAL DO MATO GROSSO e vencido pela empresa TELTEC SOLUTIONS LTDA.

- O objeto licitado foi APPLIANCE FÍSICO.

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Web Application Firewall e Balanceamento de Carga	2	R$ 525.000,00	R$ 1.050.000,00
2	Serviço de instalação e configuração da Solução de Web Application Firewall e Balanceamento de Carga	1	R$ 45.000,00	R$ 45.000,00
3	Capacitação	4	R$ 24.950,00	R$ 99.800,00
TOTAL				**R$ 1.194.800,00**

FONTE 2:

A tabela abaixo diz respeito ao valor registrado no Item 5 do Pregão Eletrônico Nº 02/2022(SRP), realizado pelo TRIBUNAL REGIONAL ELEITORAL DA BAHIA, cujo objeto foi "SOFTWARE DE BALANCEAMENTO DE CARGA COM FIREWALL DE APLICAÇÕES", com garantia e suporte do fabricante por 60 (sessenta) meses, com vencedor LANLINK SOLUCOES E COMERCIALIZACAO EM INFORMATICA S/A.

- O objeto licitado foi APPLIANCE VIRTUAL.

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
5	Solução de Web Application Firewall e Balanceamento de Carga	2	R$ 498.000,00	R$ 996.000,00
TOTAL				**R$ 996.000,00**

FONTE 3:

A tabela abaixo diz respeito ao valor pago pela solução contratada através do Contrato no 28/2019, referente ao Pregão Eletrônico 00015/2019, realizado pelo MINISTÉRIO DA EDUCAÇÃO (MEC) e vencido pela empresa MJP INFORMATICA E SERVICOS LTDA, cujo objeto foi "AQUISIÇÃO DE SOLUÇÃO DE SEURANÇA DA IINFORMAÇÃO APPLICATION DELIVERY CONTROLLER (ADC), COM FUNÇÕES DE BALANCEADOR DE CARGA E ACELERAÇÃO WEB COM MÓDULOS DE LOADING BALANCE, GLOBAL SERVER LOADING BALANCE, WEB APPLICATION FIREWALL E SSL OFFLOAD E INSPECTION (LB/GSLB/WAF/SSL), INCLUINDO GARANTIA DE 60 (SESSENTA) MESES E SERVIÇOS AGREGADOS DE INSTALAÇÃO, TREINAMENTO E SUPORTE TÉCNICO ESPECIALIZADO".

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Cluster de Solução de Segurança da Informação Application Delivery Controller (ADC), com funções de balanceador de carga e aceleração web com módulos de Loading Balance, Global Server Loading Balance, Web Application Firewall e SSL offload e inspection (LB/GSLB/WAF/SSL), incluindo garantia de 60 (sessenta) meses	1	R$ 1.933.000,00	R$1.933.000,00
2	Serviços de definição do projeto, implantação, instalação e configuração da solução contratada (ITEM 1)	1	R$46.000,00	R$46.000,00
3	Treinamento (40 Horas)	1	R$46.916,00	R$46.916,00
4	Suporte Técnico Especializado para toda a solução descrita no ITEM 1 contemplando atualização de versões, patchs e correções de bugs, suporte presencial (on-site) 24x7 e suporte programático, pelo período de 36 (trinta e seis) meses.	36	R$4.819,44	R$173.499,84
TOTAL				R$ 2.199.415,84

FONTE 4:

A tabela abaixo diz respeito aos valores dos itens 1 a 7 referentes Pregão Eletrônico 046/2021, realizado pelo TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO e vencido pela empresa ADD VALUE PARTICIPACOES, COMERCIO E SERVICOS DE INFORMATICA.

- O objeto licitado foi APPLIANCE FÍSICO.

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
1	Appliance Balanceador de Aplicação	2	R$ 485.000,00	R$ 970.000,00
2	Solução de Gerenciamento.	1	R$ 100.000,00	R$ 100.000,00
3	Serviço de implantação/migração da solução.	1	R$ 44.624,45	R$ 44.624,45
4	Serviço de Suporte Técnico - Quant (48 (quarenta e oito) meses).	1	R$ 500.000,00	R$ 500.000,00
	Serviço de Suporte Técnico			

5	Especializado - Quant 300 (trezentas) horas.	1	R$ 67.500,00	R$ 67.500,00
6	Serviço de Treinamento Oficial da Solução - Quant 4 (participantes).	1	R$ 135.814,00	R$ 135.814,00
7	Serviço de Garantia da Solução - Quant 48 (quarenta e oito) meses.	1	R$ 990.000,00	R$ 990.000,00
TOTAL				R$ 2.807.938,45

FONTE 5:

Já a tabela abaixo diz respeito ao preço pago pela solução contratada através do Contrato no 132/2020, proveniente do Pregão Eletrônico 026/2020, realizado pelo MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. O objeto desta contratação foi descrito como contratação de solução de ativos de rede e balanceamento de carga para os Data Centers, incluindo serviços especializados, aquisição de equipamentos e softwares, modernização e expansão da capacidade atual para atendimento das necessidades do Ministério da Justiça e Segurança Pública.

O objeto licitado foi APPLIANCE FÍSICO.

ITEM	DESCRIÇÃO	QTDE	VALOR UNITÁRIO	VALOR TOTAL
14	Solução de segurança e balanceamento de carga – Appliance Físico – Tipo A	2	R$1.324.850,00	R$2.649.700,00
17	Operação Assistida	1	R$89.781,02	R$89.781,02
TOTAL				R$ 2.739.481,02

Como se pode observar, o orçamento estimado é o valor de R$ 2.993.303,17, obtido a partir da média de valores totais unitários das fontes mencionadas. Vale ressaltar que encontramos apenas 1(um) Edital recente para cada um dos itens "Appliance tipo físico" e "Operação Assistida", cujas fontes estão indicadas no quadro a seguir, no entanto, entendemos, s.m.j, que esse fato não prejudica a estimativa da contratação, uma vez que se pretende aferir estimativa do valor médio total da Contratação.

	TRIBUNAL REGIONAL ELEITORAL DO MATO GROSSO	**TRIBUNAL REGIONAL ELEITORAL DA BAHIA**	**MINISTÉRIO DA EDUCAÇÃO**	**TRIBUNAL DE JUSTIÇA DO ESTADO DO RIO DE JANEIRO**	**MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA**	**MÉDIA**	**QTDE**	**TOTAL**
APPLIANCE FÍSICO	R$ 525.000,00	--	R$ 966.500,00	R$ 485.000,00	R$ 1.324.850,00	R$ 825.337,50	2	R$ 1.650.675,00
APPLIANCE VIRTUAL	--	R$ 498.000,00	--	--	--	R$ 498.000,00	2	R$ 996.000,00
Serviço de instalação e configuração	R$ 45.000,00	--	R$ 46.000,00	R$ 44.624,45	--	R$ 45.208,15	1	R$ 45.208,15
Treinamento	R$ 24.950,00	--	R$ 46.916,00	R$ 33.953,50	--	R$ 35.273,17	6	R$ 211.639,00
Operação Assistida	--	--	--	--	R$ 89.781,02	R$ 89.781,02	1	R$ 89.781,02
VALOR TOTAL ESTIMADO								**R$ 2.993.303,17**

Deste modo, considerando que se trata de uma previsão do valor da contratação para efeito de estudos preliminares, o valor médio constatado para cada item pretendido, bem como a estimativa de preços total apresentada, é compatível com o preço praticado pelo mercado.

VI. ESCOLHA E JUSTIFICATIVA DO OBJETO

Inicialmente, cumpre salientar que foi avaliado a possibilidade da aderir a atas de registro de preço para adquirir o objeto, reconhecida a necessidade da proteção desses ativos e avaliando-se sempre o que seria mais vantajoso para o Tribunal em termos de qualidade da solução e o custo/benefício. A possibilidade de adesão a atas RP, justifica-se devido à urgência da contratação, em virtude do grande impacto que poderia ser gerado para os magistrados e servidores do Tribunal devido a ataques cibernéticos que estão se tornando cada vez mais comuns no Poder Judiciário e a crescente necessidade de ampliar a proteção para os sistemas e equipamentos servidores. Deste modo, a equipe de planejamento realizou extensa busca no SIASG/COMPRASNET a procura de atas de registro de preços vigentes e com sistemas compatíveis às demandas elencadas, entretanto, concluiu-se que não existem atas de Registro de Preço de entes Federais disponíveis para adesão.

Por esse motivo, a equipe de planejamento optou para que o processo de aquisição seja feito via Pregão Eletrônico - Sistema de Registro de Preços, na modalidade contratação conjunta com a participação de outros Tribunais Regionais Eleitorais interessados (Intenção de Registro de Preços - IRP), condicionado à aprovação mediante consulta prévia via Ofício-Circular.

De outra banda, em razão da análise objetiva, onde foram ponderados os pesos para os vários aspectos desejados de cada solução (SOLUÇÃO 1 / SOLUÇÃO 2), concluiu-se da inviabilidade da adoção de soluções baseadas em Software Livre (SOLUÇÃO 2) para o escopo considerado no projeto em questão. Ademais, conforme verificado no item I

deste estudo, há no mercado vários fabricantes cujos canais e representantes também atuam como integradores da solução de WAF, realizando serviços de implantação e treinamento técnico especializado, resultando em quantidade razoável de licitantes para fornecimento da solução.

Quanto aos demais requisitos gerais e modalidade de fornecimento da solução, após pesquisa junto aos TREs interessados na contratação, chegou-se ao seguintes requisitos:

1) A Solução deverá possuir gerenciamento e armazenamento dos dados na rede local do tribunal, com appliances próprios localizados e instalados na infraestrutura do cliente (on-premise). Não serão aceitas soluções baseadas em nuvem.

2) A solução deve ser licenciada para uso perpétuo. As funcionalidades da solução devem permanecer ativas após o período de garantia mesmo que desatualizadas e com todas as atualizações e assinaturas que forem disponibilizadas até data final do período que foram aplicadas ou instaladas na solução.

3) O Edital de Licitação deverá conter itens de appliance WAF na modalidade Físico e Virtual, objetivando atender necessidades específicas de cada Tribunal partícipe.

4) O Appliance físico deverá possuir interfaces LAN 10GbE, para conectividade à Rede do Tribunal.

5) Todos os Regionais consultados já possuem algum tipo de infraestrutura de containers em seu ambiente de Data Center para publicação de aplicações. Portanto, a solução deverá possuir recursos de proteção a este ambiente.

6) O fornecimento deverá prover suporte e garantia para 1 cluster que compõe a solução de WAF (Web Application Firewall) pelo período de 60(sessenta) meses.

7) A contratação deverá contemplar serviços de instalação da solução, treinamento técnico especializado e serviço de operação assistida.

VII. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA (Art. 14, IV)

Após estudos de mercado, conclui-se que a Solução 1 “Web Application Firewall - WAF baseado em Solução de Mercado” demonstrou ser opção mais vantajosa sob a perspectiva econômica e técnica, assim como a melhor escolha para alcançar os objetivos que este órgão pretende para a aludida contratação. A integração das tecnologias indicadas é capaz de oferecer todos os recursos elencados e avaliados neste estudo técnico dentro de uma mesma arquitetura de hardware/software, otimizando assim os investimentos adicionais em licenciamento e capacitação do time responsável. No mais, verificou-se que a SOLUÇÃO 1 atende adequadamente às demandas de negócio da instituição, assim como, os benefícios pretendidos são adequados e os custos previstos são compatíveis com os praticados pelo mercado.

O estudo demonstrou que os principais fabricantes destas tecnologias oferecem soluções de appliance físico e virtual, conforme requisitos do negócio, integradas através de módulos ou licenças mantendo a gestão da solução através de gerência centralizada. A utilização deste tipo de solução já é bastante difundida em instituições públicas o que comprova sua eficácia.

Para tanto, visando a consecução dos objetivos da contratação, pretende-se realizar a licitação na modalidade registro de preços, para eventual e futura a aquisição de solução de Web Application Firewall (WAF), com características de balanceamento de carga, incluindo prestação de serviços de instalação e configuração, treinamento especializado e serviço de operação assistida, com garantia técnica de 60 (sessenta) meses, de acordo com as especificações e quantitativos necessários e previstos no planejamento da contratação.

O quadro a seguir demonstra os itens necessários à contratação, com as respectivas quantidades.

GRUPO 1 - SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF)			
ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANT.
1	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE VIRTUAL, COM GARANTIA DE 60(SESSENTA) MESES.	UN	2
2	FORNECIMENTO DE SOLUÇÃO DE WEB APPLICATION FIREWALL(WAF), DO TIPO APPLIANCE FÍSICO, COM GARANTIA DE 60(SESSENTA) MESES.	UN	2
3	CAPACIDADE ADICIONAL PARA SOLUÇÃO EM FIREWALL DE APLICAÇÕES WEB	UN	2
4	IMPLANTAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	UN	1
5	TREINAMENTO ESPECIALIZADO	UN	6
6	SERVIÇO DE OPERAÇÃO ASSISTIDA	UN	1

Conforme demonstrado anteriormente, a contratação da solução de WAF (Web Application Firewall) é composta por um cluster (2 equipamentos), com seus respectivos hardwares, softwares, licenciamentos; ou fornecidos como appliance virtual. O suporte, tanto do fabricante quanto do parceiro, devem ser fornecidos no modelo 24x7 (24 horas por dia, 7 dias na semana), com garantia e serviços técnicos especializados, além de treinamento para membros da equipe que vão trabalhar diretamente na solução contratada. Abaixo seguem as principais funcionalidades listadas que serão licenciadas pelo período de 60(sessenta) meses:

1. Balanceador de Carga (ADC).
2. Global Server Load Balancing (GSLB).

3. Proteção para Aplicação.
4. Proteção Ataque DDoS.
5. DNS Application Firewall.
6. Inspeção SSL (decriptar / encriptar).

As despesas para aquisição do objeto correrão por conta dos Elementos de Despesa 44.90.40 - EQUIPAMENTOS DE TIC - SEG. INFORM. (SIN EQUTIC) e 33.90.40 - APOIO TECNICO E OPERACIONAL DE TIC (TIC APOIO), correspondente aos exercícios associados à vigência da ata de registro de preços.

VIII. LISTA DE POTENCIAIS FORNECEDORES

- G3 Solutions
  - vendas@g3solutions.com.br
  - http://www.g3solutions.com.br/
- Nome: SUPORTE INFORMÁTICA
  - http://www.suporteinformatica.com
  - andre.brasileiro@suporteinformatica.com
- TELTEC SOLUTIONS LTDA
  - e-mail teltec@teltecsolutions.com.br
  - www.teltecsolutions.com.br
- NTSEC Network Security
  - https://www.ntsec.com.br/
  - vendas@ntsec.com.br
- Nome: SWT
  - Sítio: http://www.swt.com.br/
  - Email: bsabino@swt.com.br
- Nome: Plugnet
  - Sítio: http://www.plugnetshop.com.br
  - Email: breno@plugnetshop.com.br
- L8 GROUP S.A.
  - suporte@l8group.net
  - Website: https://www.l8group.net
- Nome: SEPROL
  - Sítio: https://www.seprol.com.br/
  - Email: simone.marocco@seprol.com.br

***

ANEXO B

I - SUSTENTAÇÃO DO CONTRATO

1) Recursos Materiais e Humanos (Art. 15, I, Res. CNJ 182/2013)

**Informar se haverá a necessidade de disponibilização por parte do órgão de materiais e/ou de recursos humanos para que a STIC possa ser sustentada após a sua implantação.*

RECURSOS MATERIAIS	**DESCRIÇÃO**
[X] NÃO SE APLICA	Não existem materiais associados, ou que devem ser fornecidos pelo Tribunal para a sustentação da Solução de TI, qual seja a contratação de solução de segurança da informação para proteção de aplicações WEB. Todos as funcionalidades, recursos devem ser plenamente contemplados e fornecidos pela contratada, seja o licenciamento para o funcionamento da solução, appliance de hardware, appliance VMs, acessórios e demais componentes que devem constar do objeto da contratação para o perfeito funcionamento da solução..
RECURSOS HUMANOS	**DESCRIÇÃO**
Analistas e técnicos integradores responsáveis pela '	A Contratada deverá fornecer para os itens de implantação e treinamento da solução profissionais capacitados e certificados na solução para execução dos seguintes serviços: • Implantação da solução, incluindo instalação e configuração no ambiente do Tribunal e repasse técnico-operacional básico da solução. • Capacitação da equipe técnica (para até 6 servidores) para administração da solução, por meio de treinamento.

2) Descontinuidade do Fornecimento (Art. 15, II, Res. CNJ 182/2013)

**Informar possíveis ações para minimizar os efeitos em caso de eventual interrupção do fornecimento parcial ou total do objeto, inclusive no que se refere aos serviços complementares e insumos contratados.*

AÇÃO	**DESCRIÇÃO**
[ ] NÃO SE	

[ ] NÃO SE APLICA	
[X] REDUNDÂNCIA	• Devem ser fornecidas 2(duas) unidades para implementação de cluster, objetivando a disponibilidade da solução; • O agrupamento dos "appliances" em configuração do tipo "cluster" do tipo ativo/ativo ou ativo/passivo; • Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência; • Deve implementar a sincronização entre os equipamentos redundantes, assegurando que não haverá "downtime" e queda de sessões em caso de falha de uma das unidades; • Deve possuir redundância de dispositivos, de maneira que, em caso de falha de um dos equipamentos, o estado de todas as conexões seja remanejado para o equipamento redundante, preservando o estado original de todas as tabelas de conexões e de persistência.
[ ] RESERVA TÉCNICA	
[ ] CONTRATAÇÃO EMERGENCIAL	
[X] LICITAÇÃO PARA NOVA CONTRATAÇÃO	• No caso de encerramento do período do suporte e garantia técnica associada aos itens 1 e 2, será deliberado pela STI, por meio de consulta de demanda, a necessidade de nova contratação da garantia técnica da solução a ser fornecida pelo fabricante, para upgrade e/ou renovação das licenças e suporte da solução..
[ ] AÇÃO DE CONTINGÊNCIA	
[ ] OUTROS	

3) Transição Contratual (Art. 15, III, a, b, c, d, e; Res. CNJ 182/2013)

**Descrever como serão realizados os procedimentos necessários para que a STIC possa ser mantida plenamente operacional, de modo a minimizar os efeitos em caso de transição ou de encerramento do contrato firmado, garantindo subsistência da STIC no órgão.*

a) [ ] NÃO SE APLICA

b) [ ] entrega de versões finais dos produtos alvos da contratação;

c) [ ] transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação;

d) [ ] devolução de recursos materiais: Ao término do contrato os equipamentos fornecidos deverão ser devolvidos à CONTRATADA mediante autorização por Ofício expedido pela CONTRATANTE, informando locais e equipamentos a serem retirados, autorizando a desinstalação dos mesmos. A contratada deverá desativar o circuito imediatamente após o recebimento da comunicação formal (Ordem de Serviço) e terá o prazo máximo de 45 (quarenta e cinco) dias para desinstalação dos circuitos e retirada dos equipamentos.

e) [ ] revogação de perfis de acesso;

f) [ ] eliminação de caixas postais;

g) [ ] Aprovação dos Planos de Implantação da Solução e Continuidade de Negócios**.**

h) [ ] Prorrogação excepcional da contratação no prazo suficiente para garantir a transição para um novo contrato, caso se faça necessário;

i) [X] Outros: A CONTRATADA assume total responsabilidade pelo sigilo das informações que seus funcionários ou prepostos venham a obter em função dos serviços prestados a CONTRATANTE, respondendo judicialmente pelos danos que eventual vazamento de informação, decorrentes de ação dolosa, negligente, imperita ou imprudente, venha a afetar a CONTRATANTE ou terceiros.

1.4 Estratégia de Independência Tecnológica (Art. 15, IV, a, b)

**Informar quais as ações a serem adotadas pelo órgão em situações de descontinuidade contratual, de modo a minimizar os efeitos em caso de transição ou de encerramento do contrato firmado, garantindo subsistência da STIC no órgão.*

1.4.1. Transferência de conhecimento (Res. 182/2013 CNJ, Art. 15, IV, a)

A transferência de conhecimento da Solução de Segurança se dará por meio das seguintes ações:

ITEM	DESCRIÇÃO	FORMA DE TRANSFERÊNCIA DO CONHECIMENTO
		Repasse de Conhecimento hands-on Características do repasse de conhecimento hands-on: as atividades de instalação deverão ser acompanhadas na modalidade hands-on, devendo a CONTRATADA: a) Efetuar o repasse hands-on com carga horária de, no

4	IMPLANTAÇÃO E REPASSE DE CONHECIMENTO HANDS-ON	mínimo, 6 (seis) horas para o repasse de conhecimento referente à integração da solução e sua implantação com a transferência das informações básicas de configuração e operação; b) O repasse de informações deverá cobrir conhecimentos mínimos necessários para administração, configuração, otimização, resolução de problemas e utilização da solução; c) A equipe técnica do Tribunal, responsável pela infraestrutura técnica deverá disponibilizar no mínimo 2(dois) e no máximo 6(seis) técnicos para o acompanhamento das atividades de hands-on. As horas do acompanhamento hands-on deverão ser distribuídas ou organizadas da melhor maneira durante as atividades de instalação/configuração, mediante proposição da equipe técnica do Tribunal, com a anuência da fiscalização do Contrato. Condições de aceitação do repasse hands-on • Não serão recebidos os serviços de hands-on prestados por profissionais que não estejam hábeis a demonstrar na prática as funcionalidades principais da solução WAF, particularmente, as atividades relacionadas à mudança de configuração e operação da solução. • A não aceitação do hands-on implicará na não aceitação da entrega definitiva do serviço (ITEM 4). • Todas as despesas de instrutor(es), deslocamento de instrutor(es) e demais itens relacionados ao repasse Hands-On, serão de responsabilidade da CONTRATADA. • A empresa Licitante deverá declarar na proposta que não realizará subcontratação para a execução dos serviços.
		Treinamento técnico especializado: Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo do treinamento cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que o(s) servidor(es) capacitado(s) possam colocar os equipamentos e softwares em produção, bem como planejar mudanças de configuração no ambiente. a) O treinamento deverá oferecer carga horária total de no mínimo 20(vinte) horas. b) Serão aceitos apenas treinamentos nas modalidades online ao vivo (EAD), podendo os treinamentos online ao vivo serem gravados, a critério da CONTRATANTE. c) A CONTRATADA deve prover capacitação técnica em turma com no mínimo 5 (cinco) e no máximo 8 (oito) participantes. d) Se o treinamento for ofertado na modalidade EAD, deverá respeitar o limite de 4 (quatro) horas por dia. e) O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA. O treinamento poderá ser composto de mais de 1(um) módulo, que deverão ser discriminados na proposta da licitante. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertados atendem os requisitos indicados no item 3.5.1.e. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade da ata de registro de preços, a contar da entrega do calendário. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização após ou antes da instalação dos equipamentos, ficando a critério da administração e baseando-se no calendário a ser fornecido pela contratada.

5	TREINAMENTO ESPECIALIZADO	É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do contratado para todos os fins. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato. A contratada deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela Contratada para realização do treinamento, atualizado e poderá estar em inglês ou português. O treinamento deve ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela contratada, para configuração e execução de exercícios práticos. • No ambiente de treinamento, os servidores indicados pelo CONTRATANTE devem ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação. • Após a conclusão da capacitação, o ambiente EAD deverá permanecer disponível ao acesso do aluno por um prazo mínimo de 12(doze) meses, sob demanda do CONTRANTE. A Contratada deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a contratada informar no certificado a carga horária e assiduidade do servidor. A Contratada deverá aplicar o Formulário de Satisfação, conforme modelo de formulário constante no Anexo III deste Termo de Referência. a) No Formulário, será utilizada escala de até 4 (quatro) pontos para cada quesito do formulário. No mínimo 70% dos participantes deverão atribuir grau igual ou superior a 3 (três), para o item avaliado ser considerado proveitoso. b) O resultado da Avaliação de Instrutor será utilizado como critério de aceitação do treinamento, devendo ser considerado pela amostra de participantes como “proveitoso” para no mínimo 04(quatro) dos 07(sete) itens avaliados; c) Caso o resultado da Avaliação de Instrutor seja considerado “não proveitoso”, o treinamento fornecido será considerado não aceito; d) Na hipótese de não aceitação, a CONTRATADA deve oferecer outro treinamento, com a mesma carga horária, com outro instrutor, sem qualquer ônus para o CONTRATANTE; e) Na hipótese de o resultado do segundo treinamento ser “não proveitoso”, o objeto será considerado não aceito, aplicando-se as sanções previstas contratualmente.

1.4.3. Direitos de propriedade intelectual (Res. 182/2013 CNJ, Art. 15, IV, b)

ITEM	DESCRIÇÃO
Arquivos de configuração, planos e *as-build* de implantação, demais artefatos associados à solução produzidos durante a fase de implantação.	O instrumento contratual deve estabelecer que os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados, pertençam à Administração; A Contratada deverá ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração.

II - ANÁLISE DE RISCOS

A análise em questão é resumida, portanto, não exaustiva e focada em aspectos diretamente ligados ao procedimento nas suas etapas de planejamento da contratação, fornecimento e gestão do contrato.

Risco: 1	Não Aprovação dos documentos do Planejamento da Contratação / documentos incompletos	
Dano(s)	Atraso no processo de contratação	
Impacto(s)	- Aumento do prazo de tramitação do processo administrativo - Ausência de solução de proteção aos sistemas do Tribunal	
Ações	Responsável	Prazo
Adotar procedimentos para que a área administrativa acompanhe a elaboração, análise crítica e revisão dos documentos, evitando envios e devoluções do processo	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	Durante todo o processo de planejamento da contratação
Reuniões com superiores para sensibilização, priorização da tramitação processual e aprovação dos documentos.		

Risco: 2	Insuficiência de recursos orçamentários/financeiros para aquisição	
Dano(s)	Atraso no processo de contratação	
Impacto(s)	- Aumento do prazo de tramitação do processo administrativo - Ausência de solução de proteção aos sistemas do Tribunal	
Ações	Responsável	Prazo
Encontrar a maneira mais vantajosa economicamente para realizar a contratação	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	Durante todo o processo de planejamento da contratação
Utilização de recursos destinados a outras aquisições para contemplar esta necessidade	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
Solicitar orçamento	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
Remanejar verbas de outros projetos previstos no plano de contratações mas que não serão executados por razões diversas	SOFC	

Risco: 3	Atraso na Aquisição	
Dano(s)	Aumento do risco em caso de inoperância Paralisação do ambiente dos sistemas e dos serviços associados.	
Impacto(s)	Inoperância parcial ou total de serviços de TIC considerados essenciais	
Ações	Responsável	Prazo
Solicitação de aceleração de trâmites internos	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	Durante todo o processo de planejamento da contratação

Risco: 4	Descumprimento de cláusulas contratuais relativas ao fornecimento da solução	
Dano(s)	• Não entrega do objeto. • Atraso na entrega do objeto • Entrega do material/serviço em divergência ao exigido no Edital. • Fornecimento incompleto dos serviços de infraestrutura de TI. • Não cumprimento dos níveis mínimos de serviço	
Impacto(s)	Inoperância parcial ou total de serviços de TIC	
Ações	Responsável	Prazo

• Definição de níveis de serviços adequados, como prazo de entrega exequível.	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	Durante o planejamento da contratação
• Definição de cláusulas relativas ao descumprimento de exigências do instrumento convocatório com aplicação multa moratórias.	EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO	
• Acompanhamento e verificação de qualidade do serviço prestado. • Incentivo à solução do desvio de qualidade por meio de aplicação de glosas e, caso haja prejuízo maior previsto nos níveis de serviço, aplicação das sanções cabíveis, de forma a coibir a incidência (ou reincidência).	EQUIPE DE FISCALIZAÇÃO	Durante a execução do contrato
• Acompanhar a execução do contrato, no que tange a instalação e configuração os equipamentos fornecidos • Dividir o fornecimento em etapas e incluir no instrumento convocatório condições que obriguem a Contratada fornecer documentação ou roteiro relativo a configuração do(s) equipamento(s) fornecido(s) ou serviços prestados. • Multa moratória pela inexecução parcial.	EQUIPE DE FISCALIZAÇÃO	Durante a execução do contrato
• Primar apenas pela demanda de atividades críticas, que envolvam disponibilidade do ambiente tecnológico.	EQUIPE DE FISCALIZAÇÃO	Durante a execução do contrato
• Incentivo à solução do desvio de qualidade por meio de aplicação de glosas e, caso haja prejuízo maior previsto nos níveis de serviço, aplicação das sanções cabíveis, de forma a coibir a reincidência.	EQUIPE DE FISCALIZAÇÃO	Durante a execução do contrato

Risco: 5	Término do contrato de garantia	
Dano(s)	• Ameaça à continuidade da proteção de dados dos serviços essenciais. • Comprometimento do funcionamento da solução	
Impacto(s)	Continuidade da contratação	
Ações	Responsável	Prazo
Providenciar nova contratação de extensão de garantia	EQUIPE DE FISCALIZAÇÃO	Durante a execução do contrato
Primar pela execução das atividades críticas, que comprometam a disponibilidade do ambiente tecnológico.	EQUIPE TÉCNICA DA STI	

Risco: 6	Prazos exíguos para execução do serviço	
Dano(s)	• Retorno do crédito adicional encaminhado pelo TSE para investimento / reaparelhamento de infraestrutura do TRE-PA • Empenhos inscritos em Restos a Pagar	
Impacto(s)	Comprometimento da execução orçamentária.	
Ações	Responsável	Prazo
Acompanhamento dos prazos processuais, objetivando evitar o atraso na tramitação da contratação.	EQUIPE DE FISCALIZAÇÃO	Durante o planejamento da contratação.
Verificar se os prazos de entrega do objeto estão condizentes com a execução para o ano fiscal, incluindo as fases de recebimento definitivo do objeto, tombamento e pagamento.	EQUIPE DE FISCALIZAÇÃO	

Documento assinado eletronicamente por **ANGELA FIGUEIREDO DA SILVA MERGULHÃO**, **Coordenadora**, em 19/04/2022, às 11:01, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANTONIO EDIVALDO DE OLIVEIRA GASPAR**, **Coordenador**, em 19/04/2022, às 14:17, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **EMERSON DIAS DA SILVA**, **Chefe de Seção**, em 20/04/2022, às 09:06, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pa.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1483788** e o código CRC **C26919E6**.

0008981-46.2021.6.14.8000 1483788v250